cnsocservices@codecnetworks.in
https://codecnetworks.com

PCI DSS report

Global security standard for entities that process, store or transmit payment cardholder data.

2025-08-20T15:26:26 to 2025-08-21T15:26:26

manager.name: wazuh-virtual-machine AND rule.pci_dss: *

Most common PCI DSS requirements alerts found

Requirement 10.2.2

All actions taken by any individual with root or administrative privileges.

Top rules for 10.2.2 requirement

Rule ID	Description
5402	Successful sudo to ROOT executed.

Requirement 10.2.5

Use of and changes to identification and authentication mechanisms including but not limited to creation of new accounts and elevation of privileges and all changes, additions, or deletions to accounts with root or administrative privileges.

Top rules for 10.2.5 requirement

Rule ID	Description
5501	PAM: Login session opened.
5502	PAM: Login session closed.
5402	Successful sudo to ROOT executed.

Requirement 10.2.6

Initialization, stopping, or pausing of the audit logs

Top rules for 10.2.6 requirement

Rule ID	Description

Rule ID	Description
503	Wazuh agent started.
504	Wazuh agent disconnected.
506	Wazuh agent stopped.

Requirement 10.2.7

Creation and deletion of system level objects

Top rules for 10.2.7 requirement

Rule ID	Description
2904	Dpkg (Debian Package) half configured.
2902	New dpkg (Debian Package) installed.
533	Listened ports status (netstat) changed (new port opened or closed).

Requirement 10.6.1

Review the following at least daily:

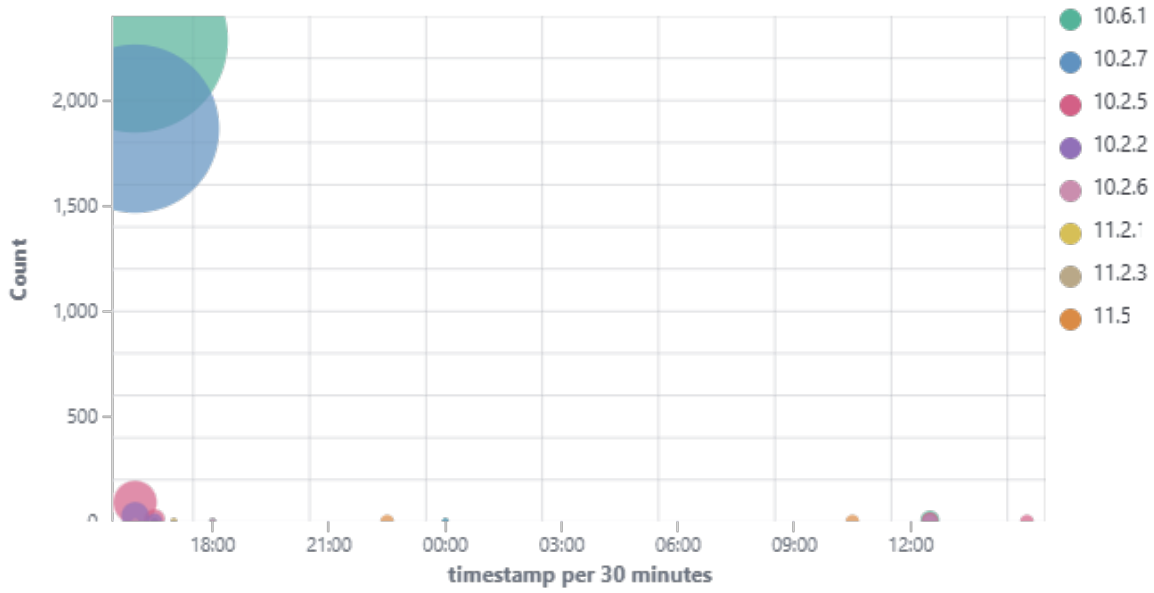
- All security events.
- Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD.
- Logs of all critical system components.
- Logs of all servers and system components that perform security functions (for example, firewalls, intrusion detection systems/intrusion prevention systems (IDS/IPS), authentication servers, ecommerce redirection servers, etc.)

Top rules for 10.6.1 requirement

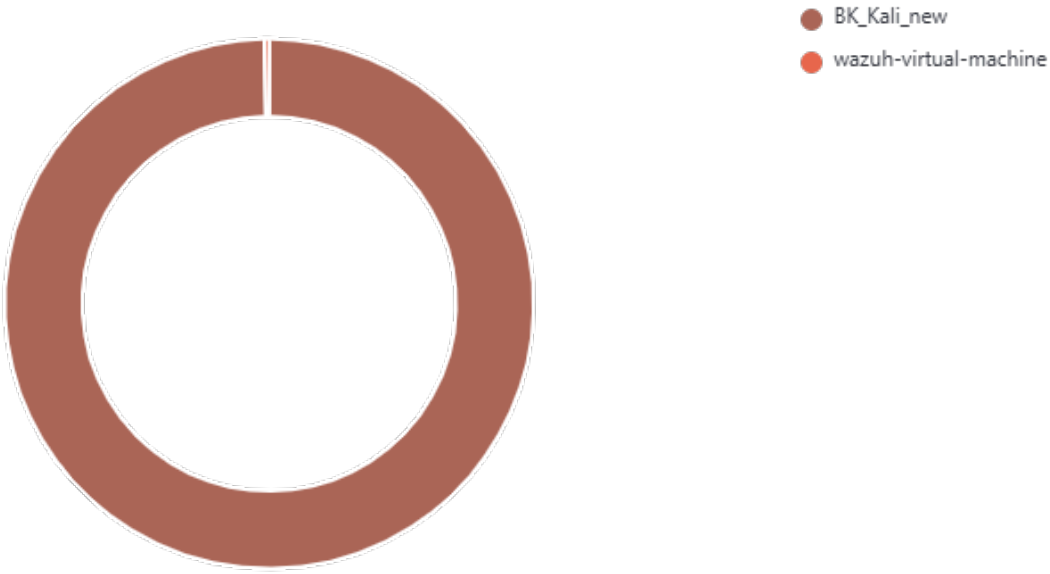
Rule ID	Description
2904	Dpkg (Debian Package) half configured.
2902	New dpkg (Debian Package) installed.
2901	New dpkg (Debian Package) requested to install.

cnsocservices@codecnetworks.in
https://codecnetworks.com

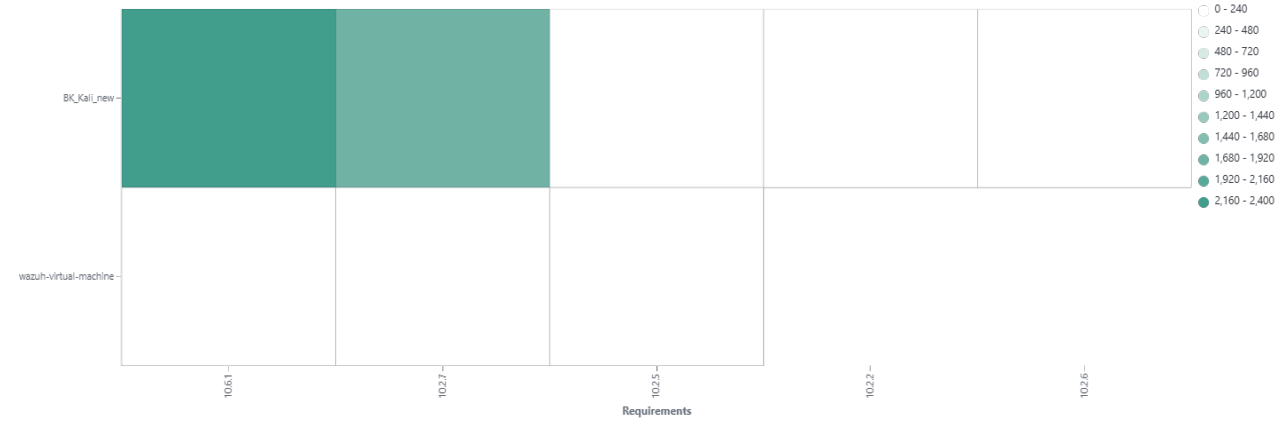
Top 10 PCI DSS requirements



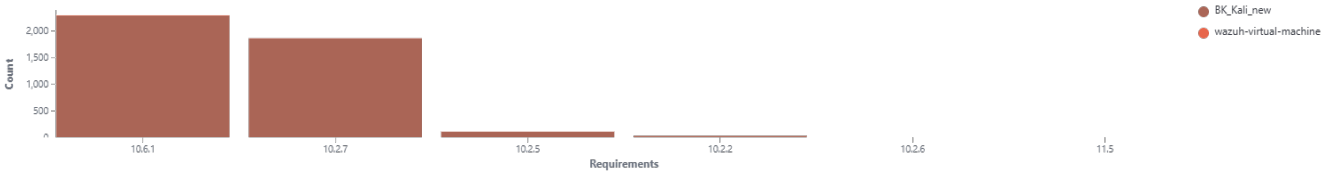
Top 10 agents by alerts count



Last alerts



Requirements by agent



cnsocservices@codecnetworks.in
https://codecnetworks.com

Alerts summary

Agent name	Requirement	Description	Count
BK_Kali_new	10.6.1	Dpkg (Debian Package) half configured.	1094
BK_Kali_new	10.2.7	Dpkg (Debian Package) half configured.	1094
BK_Kali_new	10.6.1	New dpkg (Debian Package) installed.	769
BK_Kali_new	10.2.7	New dpkg (Debian Package) installed.	769
BK_Kali_new	10.6.1	New dpkg (Debian Package) requested to install.	415
BK_Kali_new	10.2.5	PAM: Login session closed.	38
BK_Kali_new	10.2.5	PAM: Login session opened.	38
BK_Kali_new	10.2.5	Successful sudo to ROOT executed.	35
BK_Kali_new	10.2.2	Successful sudo to ROOT executed.	35
BK_Kali_new	10.6.1	Host-based anomaly detection event (rootcheck).	12
BK_Kali_new	10.6.1	Listened ports status (netstat) changed (new port opened or closed).	4
BK_Kali_new	10.2.7	Listened ports status (netstat) changed (new port opened or closed).	4
wazuh-virtual-machine	11.5	Integrity checksum changed.	4
BK_Kali_new	10.6.1	Wazuh agent started.	2
BK_Kali_new	10.2.6	Wazuh agent started.	2
wazuh-virtual-machine	10.2.5	PAM: Login session opened.	2
BK_Kali_new	10.6.1	Dpkg (Debian Package) removed.	1
BK_Kali_new	10.6.1	Wazuh agent disconnected.	1
BK_Kali_new	10.6.1	Wazuh agent stopped.	1
BK_Kali_new	10.2.7	Dpkg (Debian Package) removed.	1
BK_Kali_new	10.2.6	Wazuh agent disconnected.	1
BK_Kali_new	10.2.6	Wazuh agent stopped.	1
BK_Kali_new	11.2.1	The CVE-2025-47278 that affected Flask was solved due to an update in the agent or feed.	1
BK_Kali_new	11.2.3	The CVE-2025-47278 that affected Flask was solved due to an update in the agent or feed.	1
wazuh-virtual-machine	10.2.7	Listened ports status (netstat) changed (new port opened or closed).	1
wazuh-virtual-machine	10.6.1	Listened ports status (netstat) changed (new port opened or closed).	1